BEST PRACTICES FOR RANSOMWARE

CASE STUDY

KIVÜ

INTRODUCTION

The rampant increase in ransomware attacks has put critical-infrastructure providers on notice. A $10 billion electric utility decided it wouldn't wait until it was victimized. It invested in a prescriptive program to strengthen its cyber readiness and resilience.

CHALLENGE

With the well-publicized attack against Colonial Pipeline in May 2021 fresh in their minds, the utility's Board of Directors was becoming increasingly concerned about how prepared their company was to identify and effectively respond to such an attack, and mitigate its potential impact. Incident Response (IR) plans were in place at both a technical and executive level, and there was an incident response retainer with a well-known digital forensics and incident response (DFIR) firm. However, the Board wasn't confident that those plans or the DFIR partner were adequately prepared to address the unique nature of a ransomware attack.

The Security Incident Response Committee turned to Kivu to understand how to best analyze the nuances of ransomware attacks, evaluate how well their IR plans were positioned for identifying and responding to an event, and determine if there were additional areas of improvement that could help limit the impact of an attack when it happened.

KIVU RESPONSE

To fully evaluate the effectiveness of the utility's IR plans and ability to respond to a ransomware event, Kivu proposed a two-phased approach comprising (1) an Incident Response Plan Assessment and (2) technical- and executive-level Ransomware Tabletop sessions. In the first phase, Kivu evaluated the customer's technical and executive IR plans against NIST 800-61, with a specific view toward use of incident-handling best practices related to ransomware. In the second phase, Kivu collaborated with multiple individuals from across the organization to develop a customized and environment-plausible ransomware attack scenario for field-testing during the two tabletop exercises.

By leveraging this two-phased approach, Kivu was able to evaluate the efficacy of the company's procedures as well as IR personnel's knowledge and ability to respond to a realistic ransomware attack.

COMPANY

Provider of electric power production, transmission and retail distribution operations to the southeastern US

SERVICES UTILIZED

- Incident Response Plan Assessment (Technical focus and Executive focus)
- Ransomware Tabletops (Technical focus and Executive focus)

RESULTS ACHIEVED

By gaining insight into how well-positioned its people and procedures were to effectively respond to a ransomware event, the utility:

- Increased Board of Directors confidence in limiting the operational and financial impact of a ransomware event
- Prepared the executive team for evaluating the pay/no-pay decision in a ransomware event, to limit financial exposure
- Enabled re-prioritization of cyber investments to yield greater ROI in ransomware protection